SFJ CO10
Provide single point of contact services for investigations into digitally related crime

Overview

This standard is about providing single point of contact services to investigations which involve or require access to data about digital communications and transactions. Single point of contact involves providing advice and guidance on what can be achieved and is permissible through analysis of communications data. It also involves accessing data on communications and individuals through open-source means. It requires understanding implications of legislation and policy related to data access, handling and dissemination.

A definition of context of digitally related crime is provided in the glossary.

SFJ CO10
Provide single point of contact services for investigations into digitally related crime

Performance criteria

You must be able to:

- P1 gather data relevant to investigations of digitally related crime in compliance with current legislation and codes of practice
- P2 analyse data relevant to digitally related crime in compliance with current legislation and codes of practice
- P3 clarify needs for support in digitally related investigations with the investigating officer concerned
- P4 use open-source methods to identify material which may support an investigation or action in accordance with legislation, and local policy
- P5 provide analysis of data gathered to those authorised to receive it
- P6 access specialist technical support for investigations requiring actions beyond own level of skills, knowledge or authority
- P7 provide tactical guidance to support planning of strategy for digitally enabled crime to ensure planned actions are lawful
- P8 assess and record risk associated with proposed strategies or actions in accordance with organisational requirements
- P9 maintain secure information systems in relation to investigations into digitally related crime
- P10 research patterns and new trends in communications technology and its uses for criminal activity to support strategies for investigation of digitally related crime

SFJ CO10
Provide single point of contact services for investigations into digitally related crime

Knowledge and understanding

You need to know and understand:

K1 how to keep up to date with changes and trends in information and communication technology and their impact
K2 how to keep up to date with changes in legislation related to the countering of digitally related crime and its impact
K3 role of technical support specialists and who to access in what circumstance
K4 law enforcement information management systems relevant to investigations
K5 legislation, codes of practices and local policy related to investigation of digital sources of evidence
K6 National Intelligence Model and its application
K7 methods of tracking information relevant to the investigation subject
K8 roles, responsibilities and limits of authority of self and others involved in investigations into digitally related crime
K9 methods for analysing and presenting data
K10 technical support services available and how to access them
K11 methods for carrying out and recording risk assessment
K12 sources of guidance for use in tactical support
K13 purpose and use of open sourced methods
K14 methods which may be used to access data and communications as part of investigation or surveillance operations

SFJ CO10
Provide single point of contact services for investigations into digitally related crime

Additional Information

Glossary

There is a variety of terms used in describing crimes involving the internet and electronic communications. The core wording seems to be inter-changeable depending on which published materials are used as the source. The core words include:

1 Cyber
2 Electronic
3 Digital
4 Technology
5 e- (as in e-crime)

This NOS predominantly uses ‘digital’ as the core word.

There are two applications of this terminology in relation to crime:

1 crime which is committed through the internet or electronic communications such as fraudulent transactions, phishing etc.

2 crimes committed against individuals or organisations in which technology may have been a tool such as grooming vulnerable people for exploitation.

SFJ CO10
Provide single point of contact services for investigations into digitally related crime

Developed by	Skills for Justice
Version number	1
Date approved	January 2013
Indicative review date	January 2018
Validity	Current
Status	Original
Originating organisation	Skills for Justice
Original URN	SFJ CO10
Relevant occupations	Police officers, single point of contact (SPOC) officers; Forensic Scientists
Suite	Countering Cybercrime
Key words	Digital evidence; internet; email; electronic communications; investigation